

ABSTRACT OF THE DISCLOSURE

A cryptographic apparatus reads, from a portable storage medium, content data and cryptographic information specifying a certain part of the content data on which cryptographic processing is to be performed, specifies the certain part in the read content data based on the read cryptographic information, and performs one of encryption and decryption on the certain part. When, for example, the content data is formed from alternating headers and variable-length data sections, the cryptographic information is a program formed from an instruction sequence. The instruction sequence has the cryptographic apparatus detect a header in the content data, read the length of the variable-length data, and perform cryptographic processing on a part of the content data between a start point and an end point, the start point being a position relative to the header position, and the end point being a value resulting from adding the length to the start point.